REMARKS/ARGUMENTS

Claims 1-6, 9-25, and 27-32 are pending. Claims 1, 9, 15, 21, and 30 have been amended. No new matter has been introduced. Applicant believes the claims comply with 35 U.S.C. § 112.

Applicant would like to thank Examiner Joseph Pan and Examiner Thanhnga B. Truong for the courteous interview extended to Applicant's counsel, Chun-Pok Leung, on October 21, 2005. During the interview, proposed amendments that would place the application in better condition for allowance were discussed. More specifically, claim amendments that would clarify the relationship between second data blocks (converted from first data blocks) and a third data block (decrypted from one of the second data blocks) in claim 30 would be favorably considered in overcoming the rejections.

Claims 1-4, 6, 9-17, 20-23, 25, and 27-32 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bojinov et al. (US 2005/0102498). Claims 5 and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bojinov et al. in view of Ashton (US 2004/0125077). The Examiner recognizes that Bojinov et al. does not teach that encrypting and decrypting are performed on the logic circuitry, and cites Ashton for allegedly disclosing the missing feature.

Claims 30-32

Applicant respectfully submits that independent claim 30 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest returning a third data block, which is decrypted from one of the plurality of second data blocks with the cryptographic criteria (which were converted from a plurality of first data blocks by encryption with the cryptographic criteria); wherein receiving a read request and returning the third data block are performed during converting the plurality of first data blocks to produce the plurality of second data blocks. In other words, a portion of the plurality of second data blocks is returned (after being decrypted as the third data block) while the plurality of first data blocks are being converted to produce the plurality of second data blocks (by encryption). The returning and the converting of the data occur in parallel.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. In FIG. 1, "if first layer 110 requests that data be written, second layer 120 may encrypt the data to be written. The data, once encrypted, is stored by or at a third layer, such as 130. This is illustrated in FIG. 1 by 121. Likewise, second layer 120 may, upon another request for services by first layer 110, such as a read request, retrieve the stored, encrypted data from layer three, decrypt it, and provide it to first layer 110." Paragraph [0014]. There is no parallel processing of writing/reading and encrypting/decrypting of the data. Ashton does not cure the deficiencies of Bojinov et al.

For at least the foregoing reasons, claim 30 and claims 31-32 depending therefrom are patentable.

Claims 1-6 and 27-29

Applicant respectfully submits that independent claim 1 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest receiving a read request during converting blocks of data to produce converted blocks of data in order to access read data from the storage system, and in response thereto accessing the read data from at least one decrypted block of data, wherein the read data is decrypted from one converted block of the converted blocks of data using the cryptographic criteria to produce the at least one decrypted block of data. In other words, a portion of the converted blocks of data is accessed (after being decrypted) while the blocks of data are being converted to produce the converted blocks of data (by encryption). The accessing and the converting of the data occur in parallel.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. There is no parallel processing of writing/reading and encrypting/decrypting of the data. Ashton does not cure the deficiencies of Bojinov et al.

For at least the foregoing reasons, claim 1 and claims 2-6 and 27-29 depending therefrom are patentable.

Claims 9-14

Applicant respectfully submits that independent claim 9 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest accessing read data from the storage device in response to a read request from the host

device, including reading a third data block and decrypting the third data block with the cryptographic criteria if the third data block is one of the plurality of second data blocks, to return the decrypted third data block to the host device, wherein the step of accessing read data is performed during the step of converting. In other words, a portion of the plurality of second data blocks is accessed (after being decrypted as the third data block) while a plurality of first data blocks are being converted to produce the plurality of second data blocks (by encryption). The accessing and the converting of the data occur in parallel.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. There is no parallel processing of writing/reading and encrypting/decrypting of the data. Ashton does not cure the deficiencies of Bojinov et al.

For at least the foregoing reasons, claim 9 and claims 10-14 depending therefrom are patentable.

Claims 15-20

Applicant respectfully submits that independent claim 15 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest a cryptographic component that is operable to receive read and write requests for data stored on the storage component, while the plurality of unconverted blocks of data are converted to the plurality of converted blocks of data, wherein the cryptographic component is further operable to process a read request by accessing read blocks associated with the read request from the storage component, wherein if a read block is one of the unconverted blocks of data, then performing a first cryptographic process on the read block to produce an unencrypted read block, wherein if the read block is one of the converted blocks of data, then performing a second cryptographic process on the read block to produce an unencrypted read block, and wherein the cryptographic component is further operable to process a write request by writing one or more write blocks associated with the write request from the storage component, wherein if a write block is to be written to a block location that contains an unconverted block, then performing the first cryptographic process on the write block prior to writing the write block, wherein if a write block is to be written to a block location that contains a converted block, then performing the second cryptographic process on the write block prior to writing the write block.

In other words, for a read request, if a read block to be accessed is one of the unconverted blocks of data, a portion of the plurality of unconverted blocks is accessed (after being decrypted as the unencrypted read block using a first cryptographic process) while the plurality of unconverted blocks of data are being converted to a plurality of converted blocks of data (by encryption); or, if a read block to be accessed is one of the converted blocks of data, a portion of the plurality of converted blocks of data is accessed (after being decrypted as the unencrypted read block using a second cryptographic process) while the plurality of unconverted blocks of data are being converted to a plurality of converted blocks of data (by encryption). The accessing and the converting of the data occur in parallel.

For a write request, if a write block is to be written to a block location that contains one of the unconverted blocks of data, the write block is written (after being processed using the first cryptographic process); or, if a write block is to be written to a block location that contains one of the converted blocks of data, the write block is written (after being processed using the second cryptographic process). The writing and the converting of the data occur in parallel.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. There is no parallel processing of writing/reading and encrypting/decrypting of the data. Ashton does not cure the deficiencies of Bojinov et al.

For at least the foregoing reasons, claim 15 and claims 16-20 depending therefrom are patentable.

Claims 21-25

Applicant respectfully submits that independent claim 21 is novel and patentable over Bojinov et al. because, for instance, Bojinov et al. does not teach or suggest during the converting, receiving and servicing a file-level read request; and during the converting, receiving and servicing a file-level write request; wherein servicing the file-level read request comprises producing one or more block-level read operations; and decrypting a corresponding block of the block-level read operation with either the first or second decryption depending on how the block was encrypted during the converting; and wherein servicing the file-level write request comprises producing one or more block-level write operations; encrypting a corresponding block of data of the block-level write operation with

the first encryption, if the block-level write operation is targeted to a block location in the storage system containing data that was encrypted with the first encryption during the converting; and encrypting the corresponding block of data of the block-level write operation with the second encryption, if the block-level write operation is targeted to a block location in the storage system containing data that was encrypted with the second encryption during the converting.

In other words, for a read request, a block (a portion) of the blocks of data is decrypted with either the first or the second decryption depending on how the block was encrypted during the converting of the blocks of data. For a write request, a block is encrypted using either the first or the second encryption depending on whether the write operation is targeted to a block location containing data that was encrypted with the first or the second encryption during the converting the blocks of data. The reading/writing and the converting of the data occur in parallel.

In contrast, the writing/reading and the encrypting/decrypting of data in Bojinov et al. occur in series. There is no parallel processing of writing/reading and encrypting/decrypting of the data. Ashton does not cure the deficiencies of Bojinov et al.

For at least the foregoing reasons, claim 21 and claims 22-25 depending therefrom are patentable.

CONCLUSION

In view of the foregoing, Applicant believes all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

Chun-Pok Leung
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
RL:rl
60621063 v1